# Digital *Signatures* INITIATIVE: AN ENTERPRISE SOLUTION OF TRUST

## Executive Summary of Findings and Recommendations

**September 2000**

Prepared for

**The Council on Technology Services**
**Commonwealth of Virginia**

By

**The COTS Digital Signatures Initiative Workgroup**

Cheryl F. Clark
Chair

R. F. "Chip" German
Vice Chair

# TABLE OF CONTENTS

*Vision for The Digital Dominion: "To create a technology environment such that every citizen in every aspect of their daily life, be it economic, educational or personal, and in every interaction with government, is fully empowered by and benefits from, the promise and potential of the Information Age."*

—Governor Jim Gilmore

## INTRODUCTION

The promise and potential of the Information Age offers a vast range of opportunities for fundamentally changing and improving the way citizens and businesses interact with government and their communities. As the "Internet Capitol of the World," the Commonwealth of Virginia (CoVa) has passed critical legislation, including the nation's first Uniform Electronic Transactions Act (UETA),and issued substantive directives to help agencies reap the benefits of conducting government business in the electronic world.

As CoVa agencies build on UETA and embrace new technologies to improve customer convenience, increase worker productivity, and benefit from significant time and cost savings, it seeks to foster an electronic environment of trust. Highly publicized events, such as identity fraud and breaches in security resulting in the compromise of confidential information, disruption of services, and destruction of data and systems, have created worldwide concerns over security of conducting business online. According to experts, distrust is the primary reason why individuals choose not to conduct transactions online—when I cannot see you, how do I know you are who you say you are?

*Digital signatures can be used to provide high levels of assurance and foster an environment of trust in the electronic world.*

**A foundation of trust.** Digital signatures are one form of electronic signatures. Digital signatures legally bind individuals to specific transactions by relying on technology (i.e., public key cryptography) and policy (i.e., rigorous registration process and criteria). Like passports, digital certificates are issued by trusted third parties, known as certification authorities (CAs), and can be used to provide high levels of assurance and foster an environment of trust in the electronic world. (See Exhibit A for more information on digital signature technology.)

**An enterprise solution.** Recognizing the necessity for and benefits of digital signatures in CoVa, the Council on Technology Services (COTS) charged the Digital Signatures Initiative (DSI) Workgroup in Winter 1999 with the following deliverables:

- The foundation of policies, practices, guidelines, and standards necessary to transition into an enterprise technical production environment.
- An enterprise technical architecture and acquisition strategy based on experience.
- A Commonwealth Bridge Certification Architecture.
- An invested knowledge and skills base for decision makers and technical staff.
- A demonstrated working solution of trust and confidence extensible to the Commonwealth public sector community, to business partners, and to the public.

**Workgroup participants and contributors.** The DSI Workgroup is comprised of representatives from five agencies, four localities, an university, and VIPNet (Virginia Interactive, Inc). The DSI Workgroup established an Audit & Assurance Team—comprised of auditors and security professionals—to identify administrative obstacles, develop a digital signatures decision model, review standards, and develop an audit and control framework.

The DSI Workgroup also benefited from the extensive knowledge and experience of CoVa employees and contractors, the vendor community, other states, the Federal government, and the Government of Canada. (See Exhibit B: DSI Participants and Contributors for more information.)

*A demonstrated working solution of trust and confidence extensible to the Commonwealth public sector community, to business partners, and to the public.*

**The process.** To get a jumpstart, the DSI Workgroup leveraged the best thinking and experiential learning of other states, the Federal government, and the private sector. The DSI Workgroup first convened in December 1999, and conducted monthly business meetings to share information on best practices and methods for overcoming barriers and obstacles. (See Exhibit C: DSI Calendar of Events for a complete accounting of the Workgroup's activities.)

The Workgroup launched eleven digital signature with public key infrastructure (PKI) demonstrations in Summer 2000, and used the lessons learned from the demonstration effort to inform its findings and recommendations. (See Exhibit D: DSI Demonstration Projects Overview for more information on the pilot programs, partners, objectives, and functions.)

The University of Virginia conducted a limited and successful demonstration of a bridge certification authority (BCA). The BCA is modeled after the federal bridge project, and cross-certifies certification authorities (CAs) to promote interoperability and expand trust domains. In other words, the holder of a certificate from one CA can conduct transactions with anyone holding a certificate from any CA cross-certified through the bridge. The Workgroup learned that the bridge simplifies the cross-certification process by removing the administrative and technical burdens from the CA pool. The bridge is one mechanism by which to promote interoperability.

The DSI Workgroup was originally chartered to explore ***if*** digital signatures should be adopted. When Executive Order 65 was released in late May, directing agencies to "take advantage of the benefits of digital signature technology to the fullest extent possible," the focus shifted to ***how*** digital signatures should be adopted. (See Exhibit E: DSI Deliverables for more information on the Workgroup's charge in relation to Executive Orders 51 and 65.)

## VISION AND GUIDING PRINCIPLES

The DSI Workgroup supports the Governor's vision for the Digital Dominion—for improved, efficient operation of government and greater convenience and delivery of government services to citizens and businesses. The DSI Workgroup envisions creating an environment of trust, interoperability, and security for individuals and businesses conducting electronic transactions with the Commonwealth of Virginia.

**Guiding principles.** The DSI Workgroup built consensus around the following guiding principles, which provided a sound framework for the subsequent recommendations:

- ***The power of attraction***. Create a voluntary, CoVa enterprise solution that will garner support and widespread use among agencies, institutions, and localities, not because it is compulsory, but because it is attractive, maximizes convenience for internal and external customers, optimizes ease of adoption and use, and makes the best business sense.
- ***A solid foundation.*** Our recommendations are framed to ensure integrity, flexibility, and maximum security balanced with the pace and scope of deployment. We want to build a solid foundation to position CoVa to take advantage of the greatest gains in the rapidly-evolving technology marketplace.
- ***Simplicity and flexibility.*** To achieve early deployment and facilitate ease of adoption and use for agencies, institutions, and localities, our recommendations aim for the simplicity of the "cleanest," least complicated and most flexible technology and policy solutions.

*The DSI Workgroup envisions creating an environment of trust, interoperability, and security for individuals and entities conducting electronic transactions with the Commonwealth of Virginia.*

## FINDINGS AND CONCLUSIONS

Our substantial body of findings, lessons learned, and best practices has led us to draw the following seven key conclusions:

1. **Trust is the linchpin of digital signature technology.** Trust is absolutely central to digital signatures: Can I trust that you are who you say you are? That my data will arrive without tampering? That your digital certificate was obtained properly and issued by a third party I can trust? The highest level of assurance is necessary to conduct trustworthy electronic transactions with confidence.

*Our recommendations are framed to ensure*

2. **Digital signatures should be used for authentication, data integrity,**

**and non-repudiation.** Digital signatures can help accomplish the following:

i. ***Authentication***—digital signatures are tied to specific identities.

ii. ***Integrity of data***—using a hashing function, digital signatures compute and compare message digests to ensure data was not altered prior to signature verification.

iii. ***Non-repudiation***—digital signatures are legally binding and are tied to specific individuals.

*integrity, flexibility, and maximum security balanced with the pace and scope of deployment.*

3. **Digital signature technology has a place in an overall security architecture.** Digital signatures are one form of electronic signing and one form of authentication. Other options—used singly or in combination—include double-clicks, passphrases and PINs, hardware tokens and smartcards, and biometrics. Digital signatures in and of themselves do not provide the basis for e-government. An absence of digital signature capability in the hierarchy of electronic signatures, however, can be an impediment to e-government.

   When issued using a stringent proof-of-identity registration model, digital signatures represent the highest level of assurance in verifying authentication, providing for integrity of data, and supporting non-repudiation. Because of the high assurance levels, digital signature technology is more complicated and costly to implement and use than other forms of electronic signatures, and may not be appropriate or practical for every application requiring a signature. For applications involving high risks and extremely sensitive data, and requiring a high level of assurance that the parties involved in the transactions are who they claim to be, digital signature solutions are unparalleled.

*Digital signatures are but one piece of an overall security architecture.*

4. **Deploying digital signature technology is not a trivial exercise.** When the Workgroup formed last year, several states seemed to be at the brink of deploying enterprise-wide digital signature solutions, and CoVa was poised to be left in the PKI dust. Though all the indicators pointed to rapid growth and use of digital signatures in 2000 and beyond, the lack of standards, interoperability issues, and legal and liability questions have been barriers to progress.

   Experts predicted that the rapidly evolving technology marketplace would push the resolution of these issues and open questions and open the floodgates to mass adoption. That has not been the case. Despite recent federal and state legislation, deployments of digital signature technology continue to be limited in size and scope. No state has moved into a full PKI production environment, and most states do not have an explicit statement of direction. Some states, such as Massachusetts, have backed away from implementing enterprise-wide PKI solutions.

   Despite claims or appearances to the contrary, our demonstration effort confirmed that digital signatures and PKI are far from being "plug and play" solutions. Implementation involves:

   - Significant investment of time, resources, and expertise;
   - A steep learning curve;
   - Substantial process reengineering;
   - Overcoming cultural, legislative, technical, and policy barriers;
   - Evolving standards;

- Interoperability issues; and
- Open questions of liability.

5. **Digital signature and electronic government deployments are subject to systemic obstacles which can create a cycle of paralysis.** Transitioning to an e-government environment turns the "business as usual" (or "government as usual") paradigm on its ear. Traditional methods of provisioning government and conducting government business—from budgeting to workflow to auditing—must be re-thought. Systemic obstacles to this re-thinking exist, such as:

   - ***Infrastructure,*** including the processes for budgeting and procuring hardware and software products and services
   - ***Cultural beliefs and practices,*** such as resistance to change, distrust of technology, lack of awareness, and reliance on outmoded systems and practices like the traditional cost justification model vs. long-term strategic, customer-centered gains.
   - ***Funding,*** to support systems change and cover substantial up-front costs.
   - ***Staffing,*** to provide horsepower for new development while continuing to maintain existing systems and services

   Effecting change in the fundamental way in which government conducts business requires breaking the cycle of systemic problems and gaining a critical mass of acceptance and support.

6. **The greatest value of digital signatures lies in associated reengineering of business processes.** Automation provides convenience and cost savings, and digital signatures themselves provide trusted authentication and identification in the electronic environment. The greatest potential value may derive from the process of reengineering workflow and applications to create a customer-oriented electronic environment. Customer transactions that currently take days to go through a manual process to complete will be redesigned to allow real-time, interactive transactions that can be completed in minutes. Digital signatures and automation present opportunities to raise standards for business processes, workflow, and security and improve and redefine best practices. We want to put a working philosophy in place that we not replicate the security and accountability weaknesses and vulnerabilities often inherent in paper-based processes as we transition these processes into the electronic world.

*The greatest value of digital signatures lies in associated reengineering of business processes and transition to best practices.*

7. **Digital signatures are connected to and can advance other CoVa initiatives and activities toward a seamless implementation of electronic government.** The progress of the DSI Workgroup interrelates with Executive Orders 51 and 65 and with other initiatives spearheaded by COTS, the Secretary of Technology, and his reporting agencies. In particular, the work of the following groups or initiatives provides specific opportunities to create synergies:

   - COTS Privacy, Security and Access Workgroup
   - COTS Enterprise Architecture/Security Workgroup
   - Department of Technology Planning
   - EO 51 E-forms and digital signatures

- EO 65 Administrative Systems
- COTS Seat Management Program
- Commonwealth Portal Strategy
- Commonwealth Kiosks

## SUMMARY CONCLUSION

Relying on the guiding principles and findings and conclusions articulated by the DSI Workgroup, CoVa should deploy digital signature and PKI technology strategically. Recognizing the legal, policy, technical, operational, cultural barriers; uncertainties related to applied case law; and the continued evolution of associated standards and products, CoVa should move forward strategically to build momentum and the infrastructure that would support a full-scale PKI production environment.

To that end, the DSI Workgroup believes CoVa should adopt an enterprise solution of trust—a solution that offers a wide array of digital signature and PKI products, provides flexibility and simplicity, and promotes interoperability. By providing an enterprise solution, agencies, institutions, and localities do not have to invest significant time and resources in developing internal digital signature expertise and security infrastructure. A standards-based enterprise solution promotes interoperability, while allowing agencies, institutions, and localities to customize and adapt the technology to meet their business needs. Similarly, by articulating those standards, entities that choose to develop their own infrastructures will know the criteria to aim for.

## RECOMMENDATIONS

The Workgroup has crafted numerous recommendations to support implementation of digital signatures. The top ten recommendations include:

1. **Issue Virginia On-Line Transaction (VOLT) Certificates.**

   To ensure interoperability, portability, and simplicity, the Workgroup recommends issuing VOLT Certificates that adopt open standards, provide high levels of assurance, and would be used for identity only. Individuals could use VOLT Certificates with participating agencies, institutions, and localities, thereby lifting substantial key management burdens from the user. Open standards are vendor-neutral, and promote interoperability among multiple CAs.

   The Workgroup recommends that VOLT Certificates should be as "clean" as possible, including identification information only. The structure of the VOLT Certificate will follow an internationally accepted structure to provide an identity certificate that can be used for multiple applications. In the initial stages of deployment, the Workgroup recommends issuing high assurance certificates only to ensure users understand the need to maintain absolute control over their private signing keys. The Workgroup recommends instituting a CoVa PIN in the place of low assurance certificates.

*CoVa should adopt an enterprise solution of trust—a solution that offers a wide array of digital signature and PKI products, provides flexibility and simplicity, and promotes interoperability.*

2. **Develop and deploy interoperability mechanisms.**

To foster a multi-layered, multiple-vendor environment, CoVa must explore and deploy interoperability mechanisms (such as bridges and meta-directories) to expand the domain of trust. High assurance certificates issued by other governmental entities—such as the U.S. Department of Defense—could be reviewed and accepted by the VOLT Governance Team to be used alongside the VOLT Certificate. The Workgroup also recommends that CoVa monitor emerging guidelines and standards at the international and national levels.

3. **Involve legal counsel that understands the technology to advise on issues of liability and legality and assists to advance the Administration's goals for The Digital Dominion.**

   It is of paramount importance to the success of digital signatures, specifically, and e-government, in general, to have expert legal advice in formulating optimal policies, procedures, and practices.

   The Workgroup recommends the Office of the Attorney General consider creating, administratively or through legislation, a Division of Electronic Government to provide dedicated advice and assistance to all agencies and institutions of the Commonwealth. This new division in the Office of the Attorney General is analogous to the Division of Consumer Counsel (sec. 2.1-133.1) and the Division of Debt Collection (sec. 2.1-133.4). The purpose of establishing a dedicated legal division is to provide the technological/legal expertise necessary to guide the Commonwealth's agencies and institutions through the cutting edge issues that characterize e-government at a pace which supports a leadership position for CoVa.

4. **The Department of Information Technology, with direction from the Secretary of Technology and the support of the Electronic Government Implementation Division (eGov), should develop and manage the procurement of digital signature-related products and services for use by agencies, institutions, and localities.**

   The Workgroup recommends out-sourcing the certification authority (CA) function to leverage industry expertise and hasten deployment. To ensure a multi-layered environment with multiple CAs, the Workgroup recommends contracting with an enterprise PKI services coordinator that will work with multiple vendor products and solutions and provide technical assistance.

   The Workgroup recommends that the RFP(s) address provisioning the following key areas:

   - CA products and services
   - Interoperability mechanisms (such as a bridge CA)
   - CoVa PIN management
   - Application and platform integration products and services
   - Education and training
   - Marketing and promotion
   - Document retention and recovery mechanisms

5. **Reconfigure the DSI Workgroup and establish the VOLT Governance**

**Team to provide governance and policy and implementation oversight.**

*The Workgroup recommends out-sourcing the certification authority function to leverage industry expertise and hasten deployment.*

DSI Workgroup membership was limited to two members from each CoVa organization participating in the demonstration pilots. The Workgroup should be reconfigured to match the new proposed deployment effort. This will include designation of a team for ongoing governance and evolution of the VOLT Certificate. The VOLT Governance Team, a body of COTS assisted by eGov, would recommend policies to the Secretary of Technology for governing the operation of digital signature implementation, as well as conduct the following:

- Develop a concept of operations document that will serve as a basis for digital signature-related RFP(s).
- Develop and recommend VOLT certification policy and practice statements, operating rules, and applications processes.
- Coordinate review and resolution of legal, policy, technical, and business issues.
- Assist the Secretariat of Technology to articulate fully CoVa's portal strategy.
- Oversee the CoVa Enterprise PKI Service Coordinator.
- Set standards for achieving interoperability.
- Monitor and respond appropriately to "horizon" issues.

6. **Provide resources and support for agency, institution, and local government adoption of PKI and digital signatures.**

The Workgroup recommends providing seed money, resources, and other incentives to promote use of digital signature technology. Though use of digital signatures will result in cost savings over time, the startup costs can be significant. The Workgroup developed a cost model that identifies the basic cost elements for implementing digital signatures:

- Hardware and software acquisition
- Consulting, installation, configuration, integration, and testing services
- Staffing and training
- Facilities
- Ongoing maintenance

Alternative pricing strategies for cost components have been identified.

7. **Connect with CoVa initiatives and activities to promote a unified, synergistic approach to electronic government implementation.**

The Workgroup recommends building on opportunities from Executive Orders 51 and 65 to boost electronic government and deploy electronic and digital signatures. Agencies and institutions should follow the Secretary of Technology's guidance per EO 51 in incorporating electronic and digital signatures into their applications. The Workgroup recommends considering administrative applications, as defined in EO 65, as candidates for digital signature technology. These processes—used by virtually every agency in the Commonwealth—include:

- Employee benefits administration
- Leave reporting and accounting

*The Workgroup*

- Travel planning and booking
- Travel reimbursement
- Motor pool reservations
- Expense reporting

8. **Launch the VOLT Early Adopters Program for agencies, institutions, and localities that are willing and capable to deploy digital signatures in a production environment.**

Modeled after the Washington Early Adopters and Illinois' Seed Certs programs, the VOLT Early Adopters Program will demonstrate success in G2G, G2B, and G2C applications, boost confidence, and build momentum for future deployments. Candidates for the program should have some of the following characteristics:

- A sound security infrastructure in place
- Human resources to support the new technology
- Interaction with a significant government or education community
- Interaction with citizens and external partners
- Funding to support additional costs
- Processes which will benefit from the application of the technology
- Applications that can be logically enabled to support interoperability
- Administrative applications from EO 65.

The outcome of the initiative will be a solid infrastructure that will support the use of digital signatures for electronic government applications in the Commonwealth of Virginia. The Workgroup recommends the following activities to ensure success:

- Ensure program is data driven with user feedback.
- Partner with agencies, institutions, local governments, the business community, and vendors.
- Development of reusable application mechanisms for use by every level of government.
- Coordinate efforts with other CoVa workgroups and initiatives.
- Work with the agencies of the Electronic Government Implementation Division to integrate resources and identify cross-agency applications.

9. **Provide education and training to build awareness about and familiarity with digital signature technology and its benefits and implementation decision factors.**

Conduct an education and awareness campaign targeted to CoVa employees in agencies, institutions, and localities; legislators; and segments of the business and citizen populations.

As stated in EO 65, the Electronic Government Implementation Division should educate agency leaders interested in or considering adopting digital signature technology, using the decision model crafted by the DSI Audit & Assurance Team.

*recommends providing seed money, resources, and other incentives to promote use of digital signature technology.*

All digital signature users should receive security awareness training for private key protection before high-assurance key pairs are issued. All digital signature users should formally acknowledge their responsibilities for protecting their private key before access to any system utilizing the high-assurance key is granted.

**10. Leverage the learning and expertise of others, and monitor emerging technologies and security solutions for applicability to CoVa.**

Because the environment continues to evolve rapidly and operates in a larger context than a single entity, region, state, or country, there are significant opportunities for linking, leveraging, and leadership on the horizon.

#### Emerging Applications and Practices

- A substantial body of federal regulations is expected in fall 2000 for securing medical records from the Health Insurance Portability and Accountability Act (HIPAA).
- National and CoVa interest in electronic notaries and in defining new roles for notaries as important components of a high-assurance digital signature registration process.
- High demand among citizens for voter registration and online voting applications, especially in congested areas and remote rural locations.
- Opportunities to provide certification authority and registration authority services to the general public are being explored internationally by banks and financial institutions. Nationally, the United States Postal Service (and their vendor IMAGITAS of Boston) envisions a pilot with federal, state and local agencies in which USPS acts as the Registration Authority.
- The Federal Access Certificates for Electronic Services (ACES) program promulgates digital certificates among federal agencies. The Federal Electronic Commerce Program is identifying cross-cutting applications—applications that transverse federal, state, and local lines.
- The California legislature is considering action which would designate the California Department of Motor Vehicles the state's Registration Authority.

*Provide education and training to build awareness about and familiarity with digital signature technology and its benefits….*

#### Evolving Standards and Technologies

- Electronic forms and workflow software
- Biometrics
- Smartcards and alternative hardware tokens
- Encryption
- Document management.
- Tools and methodologies which could enable Single Sign On (e.g., directory structures, attribute certificates, privilege management frameworks, etc.)

## PLAN OF ACTION

The DSI Workgroup recommends the following action steps.
(See Exhibit F: Time-Phased Workplan.)

*…there are significant opportunities for linking, leveraging, and leadership on the*

*horizon.*

1. The Secretary of Technology should reestablish the Digital Signatures Workgroup to consist of the VOLT Governance Group, the DS Procurements Team and other sub-units to support the proposed deployment effort. The new DS Deployment Workgroup should oversee the RFP development process and coordinate the resolution of legal, policy, and technical issues

   ***Timeframe: October 2000***

2. DIT should procure a vendor source or sources for an array of enterprise products and services related to PKI and digital signatures, including CA services (prominently featuring VOLT-standard products) and all based on DSI findings and recommendations. DIT should work with the DS Deployment Team to develop a concept of operations and articulate the VOLT open standards. Applications and platform integration services should be procured in the same manner.

   ***RFP Development: October 2000 – January 2001***
   ***Issue RFP(s): January 2001***
   ***Award RFP(s): June/July 2001***

3. The standards and best practices recommended by the DSI Workgroup should be adopted through the Secretary of Technology, most notably those applying to the VOLT Certificate, its assurance levels, audits and controls, storage of private keys, and recommended limits on the use of document encryption for storage.

   ***October 2000***

4. A source of funding should be sought by the Secretary of Technology.

   ***October 2000***

5. Appropriate staffing should be supplied for the effort through the Secretary of Technology, most notably legal counsel and project management.

   ***October –November 2000***

6. The proposed digital signature deployment timeline should be adopted by and promoted as a priority to Secretary of Technology agencies.

   ***October 2000 – January 2001***

7. Early Adopter candidates—Executive Order 65 administrative applications, agencies, localities, and the educational community—should be recruited selectively by the Digital Signature Deployment Workgroup and commissioned by the Secretary of Technology.

   ***October 2000 – January 2001***

8. The COTS Executive Committee should proactively exploit synergies the Digital Signature Initiative has identified with other COTS initiatives and align priorities and resources to boost momentum toward the Administration's vision for the Digital Dominion.

   ***October 2000 and ongoing***

9. The Department of Technology Planning and the Electronic Government Implementation Division should develop a training program and a promotional and security awareness campaign which takes advantage of the DSI findings and lessons learned.

   ***October 2000 – January 2001***

10. The DS Deployment Workgroup should actively monitor ‘horizon’ issues and work through COTS to adjust for and to leverage these developments.

***October 2000 and ongoing***

## TOOLS AND RESOURCES

As a result of the DSI effort, we have developed a number of tools and guidelines, and developed a substantial base of knowledge to advance CoVa toward the Governor’s vision for The Digital Dominion. In particular, we have:

### Solutions

- A simplified, vendor-neutral trust architecture model based on open standards.
- A flexible business model to guide implementation of digital signatures that can meet the needs of CoVa as an enterprise as well as the needs of its disparate organizational components.
- Principal role definitions for moving forward in a coordinated, strategic manner with multiple partners.
- An acquisition strategy with selected supporting reference materials to inform and guide deployment decisions.
- A plan of action synergistic with other COTS endeavors and initiatives at all levels in the public and private sectors.
- An enterprise solution to offer agencies, localities, and higher education that provides the best business case for adopting digital signature technology.

### Tools

- Step-by-step business decision criteria to guide decision-makers in determining whether digital signature technology is appropriate.
- A cost model that highlights direct and opportunity costs, and the major cost considerations in deploying digital signature technology.
- Audit and assurance best practices and standards to ensure proper controls are put into place to protect transactions, prevent fraud, and provide an audit trail.
- Key technical standards to promote interoperability and provide high levels of assurance.

### Resources

- Experience-based knowledge and skills developed through the robust demonstration effort and by building on the knowledge and experiences of others nationally and internationally.
- An informed perspective on evolving issues and trends.
- Contacts in multiple states, the federal government, and the Government of Canada.
- Strong industry relationships with digital signature and PKI vendors and experts.

**Conclusion.** As a result of the DSI Workgroup's inquiry, CoVa is positioned to assume a leadership role in deploying digital signature technology strategically to improve services to citizens, realize cost-savings benefits, and reap the benefits of electronic government.

*A simplified, vendor-neutral trust architecture model based on open standards.*

*As a result of the DSI Workgroup's inquiry, CoVa is positioned to assume a leadership role in deploying digital signature technology strategically to improve services to citizens, realize cost-savings benefits, and reap the benefits of electronic government.*

EXHIBIT A

# INTRODUCTION TO DIGITAL SIGNATURES

In conducting business in the physical world, we rely on established patterns of trust to guide our decisions. We have long-standing trust relationships with our retailers, employers, and government agencies. In the physical world, there is tangible evidence of identity—storefronts, nametags, state-issued identity cards, licenses, and other credentials—to provide reasonable assurance that the parties can be trusted; that they are who they say they are.

In the electronic world, we do not have the same trust cues to follow—we cannot "see" whom we are dealing with or know whether they are properly licensed or authorized to handle our transactions. The electronic world relies on a blend of technology and policy to establish trust relationships. One of the most powerful trust mechanisms is digital signature technology.

Having the same legal ramifications as pen-and-ink (or "wet") signatures, digital signatures are a string of numbers computed mathematically and attached electronically to a record to indicate the intent to sign the record. Because digital signatures employ public key cryptography, they are much more powerful than a wet signature. Digital signatures:

- Are tied to specific individuals and are legally binding;
- Protect the confidentiality of data;
- Ensure that data has not been tampered with since it was signed; and
- Prevent individuals from falsely repudiating transactions.

## PUBLIC KEY CRYPTOGRAPHY

Cryptography has its roots in ancient history—Julius Caesar supposedly created one of the earliest cryptographic systems to communicate secret messages with his warriors. Until the invention of public key cryptography, people relied on ***symmetric cryptography***. Caesar and his men, for example, used the same ***key*** to encrypt (scramble) and decrypt (unscramble) messages. One significant problem with this model is that—at some point—the key would have to be transported across geo-political boundaries and could thus be compromised. In addition, if Caesar corresponded with multiple warriors in many different parts of the empire, he may wish to have different codes for each to increase security. These men, in turn, would have to share keys to correspond among themselves. As the number of users increases, the number of keys to manage increases dramatically.

**Key pairs.** Public key cryptography—a recent invention—relies on two separate but interrelated keys and is known as ***asymmetric cryptography***. Keys come in mathematically related pairs—a public key and a private key. The public key can be distributed publicly without compromising the integrity of the private key—the private key cannot be derived from the public key. The private key must be kept secret and assigned to a single individual. Any data signed by the private key can ***only*** be unlocked or verified by the corresponding public key. Similarly, any encryption performed by the public key can only be decrypted by the corresponding private key. Because significantly fewer keys are involved in a network environment, key management is greatly simplified.

## CRYPTOGRAPHY AND DIGITAL SIGNATURES

Digital signatures rely on public key cryptography to provide security, assure data integrity and confidentiality, and support non-repudiation. To understand how cryptography and digital signatures work in the electronic environment, the following example illustrates how to write and send a digitally signed check.

**Security.** Suppose you want to write a check, requesting your bank to pay a specific amount to a specific individual. When it comes time to send your check over insecure lines, you encounter several serious security problems:

- Someone could intercept or "sniff" your check and learn valuable information about you, such as your account number, contact information, and the specifics of your transaction, so you need confidentiality.
- Someone could falsely assume your identity and create similar, counterfeit checks, so the bank needs to verify that it was you who wrote the check.
- Someone could intercept your check and alter it, so the bank needs to know that the check has not been tampered with since you sent it.
- You could deny ever creating the check, so the bank needs non-repudiation.

Digital signatures solves these security problems. Most of the digital signature functions occur automatically in the background—the user follows a series of simple steps and questions, and is alerted if there is a breach in security. Here's a behind-the-scenes look at how digital signatures works.

1. **Sign.** The first step to digitally signing the check is creating an "electronic fingerprint" or ***hash code*** of the check. If a single letter or digit of the message is changed, the hash code will change dramatically, alerting the recipient that the data may have been tampered with. Use your private signing key to sign the hash code of the check, and append the signed hash code to the check.

2. **Seal.** To ensure the confidentiality of the check and ensure that the recipient is the only individual capable of opening your check, you should "seal" or encrypt the check. Public key cryptography can be used to encrypt documents, but it is unwieldy and slow, and is intended to encrypt small amounts of data. Symmetric key cryptography is designed to encrypt large quantities of data quickly. Because symmetric keys do not offer high assurance levels, it is important to use a combination of public key and symmetric key cryptography to seal your check.

   In this example, create a one-time symmetric key to encrypt the check. Once it has been encrypted, use the ***recipient's*** public key to encrypt the symmetric key. Why use the recipient's public key? The only key that can decrypt the recipient's public key (and thus the symmetric key) is the recipient's ***private*** key, to which only the recipient has access. If you used your private key to encrypt the symmetric key, your public key—which anyone can access through a directory service—can decrypt the symmetric key. By using the recipient's public key, you can be certain that the recipient is the only individual who can decrypt and read your check.

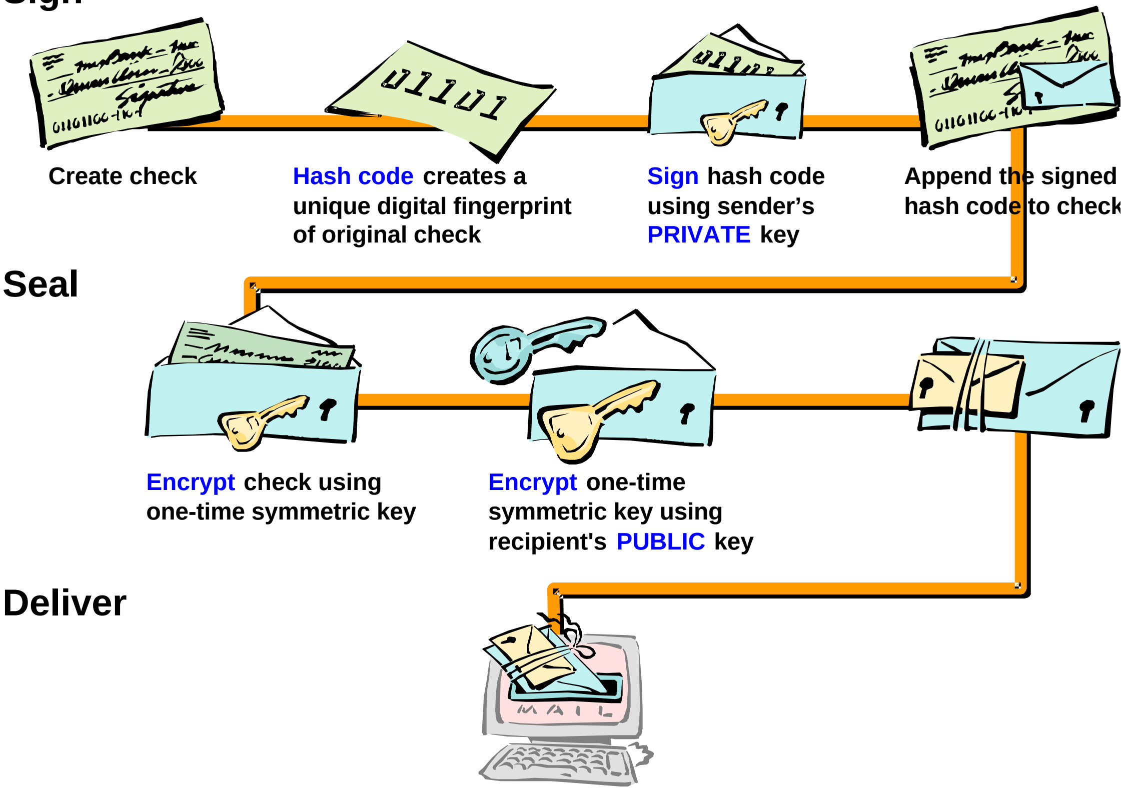
3. **Deliver.** Submit the signed hash code of the check, the encrypted check, and the protected encryption key to the recipient electronically.

4. **Accept.** The check and the accompanying materials arrive to the recipient.

5. **Open.** The recipient uses his or her private key to decrypt the one-time symmetric key. The recipient then decrypts the check.

6. **Verify.** To verify the identity of the sender, the recipient would use the sender's public key to decrypt the hash code of the check—the digital signature. A new hash code of the check is computed and compared to ensure the data was not altered prior to verification.

**EXHIBIT A**



## Sign

Create check

Hash code creates a unique digital fingerprint of original check

Sign hash code using sender's PRIVATE key

Append the signed hash code to check

## Seal

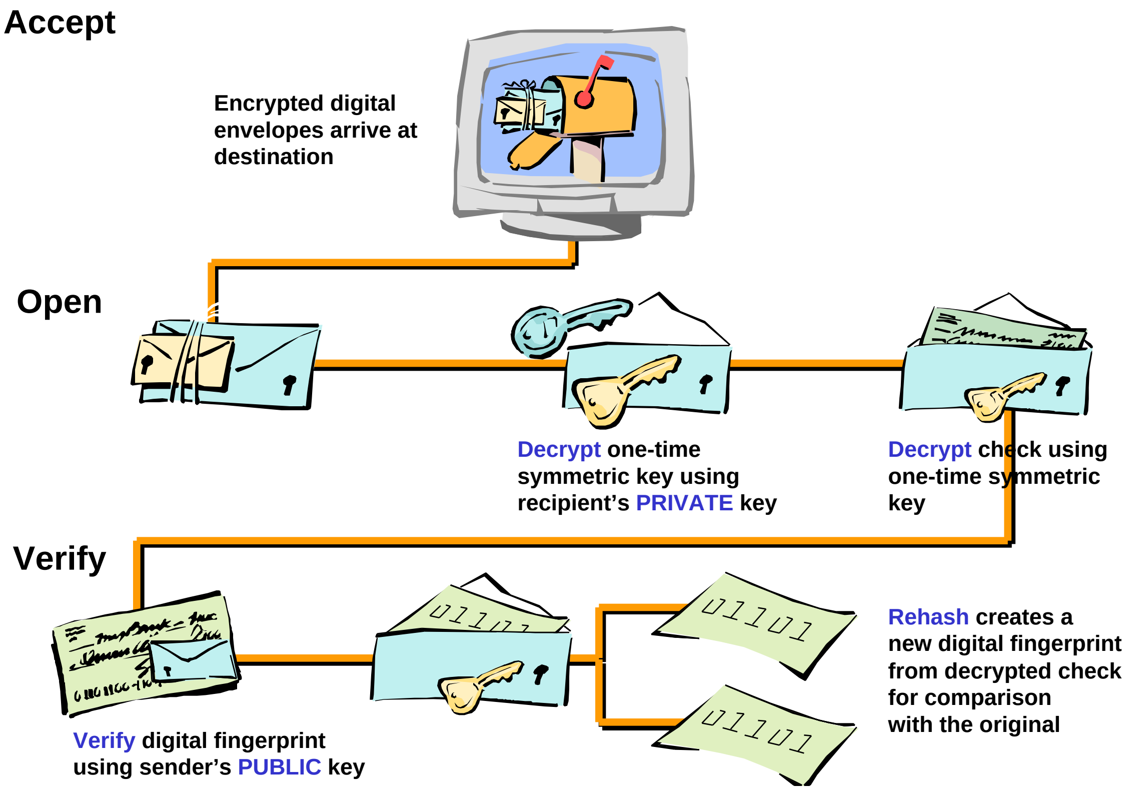
Encrypt check using one-time symmetric key

Encrypt one-time symmetric key using recipient's PUBLIC key

## Deliver

Mail electronic envelopes to recipient

# EXHIBIT A



Accept

Encrypted digital envelopes arrive at destination

Open

Decrypt one-time symmetric key using recipient's PRIVATE key

Decrypt check using one-time symmetric key

Verify

Verify digital fingerprint using sender's PUBLIC key

Rehash creates a new digital fingerprint from decrypted check for comparison with the original

EXHIBIT B

# DIGITAL SIGNATURES INITIATIVE WORKGROUP

## MEMBERS

Jim Adams
Sr. Information Technology Manager
Department of Information Technology

David Bunn
Network Systems Supervisor
Department of Motor Vehicles

Charles Cassaro
Team Supervisor
City of Norfolk

Cheryl Clark (Chair)
Chief Information Officer
Department of Motor Vehicles

Jan Fatouros
Director of Information Systems & Services
Department of General Services

Chip German (Vice Chair)
Director of Policy & Planning
University of Virginia

Sandy Graham
Data Security Administrator
County of Chesterfield

Diane Horvath
Director of Marketing
Virginia Interactive, LLC

Jack Kennedy
Clerk of the Court
County of Wise

Virgil Kopf
CIO Information Management Systems
Department of Game & Inland Fisheries

Ray Lindquist
Vice President - Business Systems
Parikh Advanced Systems for
Department of Transportation

Tom Loper
Applications Development Specialist
Virginia Information Providers Network

Jim MaGill
Information Protection Manager
County of Fairfax

Dave Molchany
Chief Information Officer
County of Fairfax

Murali Rao
Director, Data Management Division
Department of Transportation

Wayne Robertson
Director, MIS Division
Department of Information Technology

Bill Russell
Deputy Director
County of Chesterfield

Tim Sigmon
Director, Advanced Technology
University of Virginia

Arnold Thielen
President, Mixnet Corporation for
County of Wise

Ron Tokarcik
Information Systems Analyst
City of Norfolk

# EXHIBIT B

## AUDIT & ASSURANCE TEAM

John Breeden
Manager, Records Analysis Section
Library of Virginia

Rick Cooke
Internal Audit Manager
Department of Transportation

Al Carpenter
Internal Audit Director
Department of Motor Vehicles

Barbara Deily (Chair)
Director of Audits
University of Virginia

Ben Herman (Vice Chair)
Internal Audit Director
Department of Information Technology

Charles Lawver
Internal Audit Director
Department of Medical Assistance
Services

Margaret Maupin
Internal Audit Director
Department of General Services

John Moore
Accounting Manager
Department of Game & Inland
Fisheries

Shirley Payne
Director, External Relations & Security
Coordination
University of Virginia

Bob Ross
EDP Auditor
County of Chesterfield

Kevin Savoy
Auditor
Auditor of Public Accounts

Ben Sutphin
Internal Audit Supervisor
Department of State Internal Auditor

Glenn Thacker
IT Internal Audit Manager
Department of Taxation

Steven VonCanon
Manager, Disbursements Review and
Fixed Assets
Department of Accounts

## STAFF

Janice Akers, Research and Project Coordination
Vivian Cheatham, Administrative Support
Cleo Rehmer, Research and Project Coordination
Jennifer Wootton, Technical Writer

# EXHIBIT B

## DSI WORKGROUP CONTRIBUTORS

Sprio Alifrangis
Baltimore Technologies

Gerry Anderson
Entrust Technologies

Emily Atkinson
Entrust Technologies

Jim Banwell
CACI

Becky Barnett
Department of General Services

Tim Bass
Virginia Retirement System

Roslynne Blake
Computer Associates

Michael Boorom
Operational Research Consultants, Inc.

Jim Brandt
VeriSign

Leslie Carter
Department of Information Technology

Phil Camero
Performance Engineering Corporation

Lisa Coates
Century Date Change Initiative Project Office

Claudine Conway
Government Technology Services, Inc.

Alan Cordaro
Computer Associates

David Corry
VeriSign

Mark Davis
Network Associates, Inc.

Mark Dennis
Operational Research Consultants, Inc.

David Dobson
Entrust Technologies

Debbie Dodson
Department of Motor Vehicles

Sally Fehn
Department of Information Technologies

Sandy German
University of Virginia

Richard Gill
RSA Security

Craig Goeller
Department of Medical Assistance Services

Debra Goodman
Computer Associates

Tom Greco
Digital Signature Trust Company

Frank Guinan
CACI for Department of Medical Assistance Services

Richard Guida
(Chair) Federal PKI Steering Committee

Gary Gumm
Parikh Advanced Systems

Michael Horkey
Unisys Corporation

John Jung
Joint Commission on Technology and Science

Lynn Kinch
Performance Engineering Corporation

Mark Kneidinger
Electronic Government Implementation Division

Yuriy Kzambasow
Digital Signature Trust Company

Chris Law
KPMG

Joe Lilly
(former) Department of General Services

Susan Martin
Department of Information Technology

EXHIBIT B

Thomas Moody
Department of Information Technology

Tim Moses
Entrust Technologies

Frederick Norman
(former) Unisys Corporation

Nick Otto
Parikh Advanced Systems

Don Parr
KPMG

Brian Pierce
KPMG

Andy Poarch
(former) Executive Director, Council on Technology Services

Lee Reams
City of Norfolk

Jake Reynolds
Department of Information Technology

Stephanie Saccone
Department of Information Technology

Rose Schooff
Library of Virginia

Lana Shelley
Department of Motor Vehicles

Lynn Sikora
Department of Game & Inland Fisheries

Prasanna Simha
Computer Associates

Ann Smith
Valicert, Inc.

Michael Snipes
Entrust Technologies

Jeff Stapleton
KPMG

David Sweigert
Entrust Technologies

Rusty Taub
RSA Security

Teresa Thomas
Auditor of Public Accounts

Danny Wasyk
County of Chesterfield

Brandon Weidner
Computer Associates

Karen West
Digital Signature Trust Company

Richard Wilhelm
County of Fairfax

Rodney Willett
Virginia Information Providers Network

EXHIBIT B

## PARTICIPATING GOVERNMENT AND INDUSTRY ORGANIZATIONS

Auditor of Public Accounts, Commonwealth of Virginia
Baltimore Technologies
CACI
Cardobe Technologies
City of Charlottesville
City of Norfolk
Computer Associates
Council on Technology Services, Commonwealth of Virginia
County of Chesterfield
County of Fairfax
County of Wise
Department of Accounts, Commonwealth of Virginia
Department of Game & Inland Fisheries, Commonwealth of Virginia
Department of General Services, Commonwealth of Virginia
Department of Information Technology, Commonwealth of Virginia
Department of Medical Assistance Services, Commonwealth of Virginia
Department of Motor Vehicles, Commonwealth of Virginia
Department of State Internal Auditor, Commonwealth of Virginia
Department of Taxation, Commonwealth of Virginia
Department of Transportation, Commonwealth of Virginia
Digital Signature Trust Company
Electronic Government Implementation Division, Commonwealth of Virginia
Entrust Technologies
Federal PKI Steering Committee
Government Technology Services, Inc.
Joint Commission on Technology & Science, Commonwealth of Virginia
KPMG
Library of Virginia, Commonwealth of Virginia
Mixnet Corporation
Network Associates, Inc.
NIC Commerce
Operational Research Consultants, Inc.
Parikh Advanced Systems
Performance Engineering Corporation
RSA Security
SAGA
Unisys Corporation
University of Virginia
Valicert, Inc.
VeriSign
Virginia Information Providers Network
Virginia Retirement System

**EXHIBIT C**

# DSI CALENDAR OF EVENTS

## 1999

### DECEMBER

**December 7 - DSI Workgroup meeting** held at DMV, Room 702 from 9 a.m. to noon.

## 2000

### JANUARY

**January 21**- **DSI Workgroup meeting** held at DMV, Room 702 from 9 a.m. to noon.

### FEBRUARY

**February 20** - **DSI Workgroup meeting** held at DMV, Room 702 from 9 a.m. to noon.

### MARCH

**March 9 - DSI Workgroup meeting** held at DMV, Room 702 from 9 a.m. to noon.

**March 15 - Education Day** held at the University of Virginia in Charlottesville from 9 a.m. to 4:00 p.m. Primary focus was on issues and questions specifically relating to the State of Virginia pilot agencies participating in the digital signature initiative sponsored by the Council on Technology Services.

### APRIL

**April 18 - DSI Workgroup meeting** held at DMV, Room 702 from 9 a.m. to noon.

**April 26 -** RSA Security hosted a free half-day **PKI Seminar** in Washington D.C.

### MAY

**May 11**- **Meeting at the Department of Game & Inland Fisheries.** This meeting was held for all pilot project participants and Entrust Technologies. The purpose of the meeting was to resolve technical questions about the pilot projects.

**May 15** - **Meeting at the Department of Information Technology.** This meeting was held for all pilot project participants. The purpose was to explan DIT's pilot project with expected project dates along with discussion of it's design and process flow.

**May 18** - **Meeting at the Department of Game & Inland Fisheries:** Bridge meeting—principal participants were UVA, VIPNet, DGIF, and an Entrust systems engineer. The purpose of the meeting was to resolve all remaining technical issues about the bridge.

**May 25 - KPMG** hosted a full-day training session for the Audit & Assurance Team on PKI/Audit & Standards Issues in Richmond, Virginia.

**May 26** - **DSI Workgroup meeting** held at DMV, Room 702 from 8:30 a.m. to noon.

### JUNE

**June 20 - DSI Workgroup meeting** held at DMV, Room 702 from 8:30 a.m. to noon.

**June 22 - Audit & Assurance Team meeting** held at DMV, Room 730E from 1-5 p.m.

**June 29 - Audit & Assurance Team** meeting held at DMV, Room 702 from 1-5 p.m.

# EXHIBIT C

## JULY

**July 6 - Audit & Assurance Team meeting** held at DMV, Room 730E from 1-5 p.m.

**July 13 - DSI Workgroup/Audit & Assurance Team meeting and Parikh demonstration** at Parikh Laboratories in Glen Allen, Virginia.

**July 18 - DSI Workgroup meeting held at DMV, Room 702 from 8:30 a.m. to noon.**

**July 20 - Audit & Assurance Team meeting** held at DMV, Room 730E from 1-5 p.m.

**July 27 - Audit & Assurance Team meeting** held at DMV, Room 702 from 1-5 p.m.

**July 27 - State Board of Election & Registrars Conference** in Williamsburg, Virginia. The focus of this conference was on electronic registrations and on-line voting. Chip German represented the DSI Workgroup.

## AUGUST

**August 3 - Audit & Assurance Team meeting** held at DMV, Room 702 from 1-5 p.m.

**August 8 - Audit & Assurance Team meeting** held at DMV, Room 702 from 1-5 p.m.

**August 10 - DSI Workgroup meeting** held at DMV, Room 702 from 8:30 a.m. to noon.

**August 17 - Audit & Assurance Team meeting** held at DMV, Room 730E from 1-5 p.m.

**August 18 - DSI full-day work session** held at DMV, Room 635 from 9-4 p.m., to consolidate issues and reach a first level of consensus on the COTS/DSI Report. Representative team (state agency, locality, education & CA's): Ray Lindquist (VDOT), Jim MaGill (Fairfax Co.), Chip German (UVA), Jim Adams (DIT), Cheryl Clark (DMV), Jennifer Wootton (DMV) and Diane Horvath (VIPNet).

**August 24 - DSI/COTS Report Team full-day work session** held at DMV, Room 505 from 9-5 p.m. Purpose of meeting was to consolidate issues, identified gaps regarding the final draft for the COTS/DSI report. Members: Cheryl Clark (DMV), Diane Horvath (VIPNet), Chip German (UVA), Ray Lindquist (VDOT), Barbara Deily (UVA), Jim Adams (DIT), Jim MaGill (Fairfax Co.), Jennifer Wootton (DMV), Mark Dennis (ORC), Karen West (DST), Tom Grecu (DST), and Yurity Dzambasow (DST).

**August 31** - **DSI Full Workgroup** met a DMV, Room 702 from 1-5 p.m. This was a half-day work session addressing closure to key findings and recommendations from the final COTS/DSI report.

## SEPTEMBER

**September 13 - Preview meeting for Secretary Upson** on the COTS Digital Signature Workgroup's findings and recommendations. The meeting consisted of a demonstration of one of the workgroup's pilots.

**September 14** - **DSI Workgroup meeting** held at DMV, Room 702 from 8:30 a.m. to noon.

**September 27 – DSI Workgroup Executive Briefing to COTS** at the COVITS Conference, Lexington, Va.

# DSI Demonstration Projects Overview

| | Business Function | Partnering Organizations | Certification Authority And Product Used | De |
|---|---|---|---|---|
| G 2 G | Electronic purchase requests and approval<br>**Will move to production environment** | **Department of Game and Inland Fisheries** | **CA:** Served as own CA<br>**Product:** Entrust<br>600 + certificates issued | Demonstrate ag requests and ap and law enforce certificates in th submissions, pe and all other ad |
| | Certification for Funds Transfer:<br>Mobile Home Sales | **DMV**<br>**Fairfax County**<br>**Chesterfield County** | **CA:** VIPNet<br>**Product:** Entrust<br>16 certificates issued | To evaluate bus signatures with transport mecha the integration c |
| | Certification for Funds Transfer:<br>Additional Rental Sales Tax | **DMV**<br>**Fairfax County**<br>**Chesterfield County** | **CA:** VIPNet<br>**Product:** Entrust<br>16 certificates issued | To evaluate bus signatures with transport mecha the integration c |
| | Information Exchange between State and Local Government<br>Parking Ticket Information | **DMV**<br>· City of Charlottesville | **CA:** VIPNet<br>**Product:** Entrust<br>8 certificates issued | To evaluate the factors make thi |
| | Secure Web-based Electronic Filing of Court Documents<br>**Will move to production environment** | **Wise County/City of Norton Circuit Court**<br>· Big Stone Gap Housing Authority<br>· Law office of Kern & Kern<br>· Notary Public<br>· Powell Valley National Bank | **CA:** DIT<br>**Product:** Verisign<br>5 certificates issued | To enable the fi Circuit Court lar remotely and ele |
| | Web-enabling state-wide telecommunications request form<br>**Will move to production environment and to G2G category** | **Department of Information Technology**<br>· DGS<br>· Virginia Employment Commission<br>· Dept. of Conservation and Recreation<br>· DGIF<br>· DMV<br>· Chesterfield City<br>· City of Norfolk | **CA:** Verisign/DIT<br>**Product:** Verisign<br>17 certificates issued | Demonstrate int agencies to elec telecommunicat mainframe prod |

# DSI DEMONSTRATION PROJECTS OVERVIEW

| | BUSINESS FUNCTION | PARTNERING ORGANIZATIONS | CERTIFICATION AUTHORITY AND PRODUCT USED | DE |
|---|---|---|---|---|
| | Electronically Managed Travel Authorization and Reimbursement | **Department of Motor Vehicles**<br>· Unisys Corporation | **CA:** Baltimore Technologies<br>**Product:** UniCERT<br>38 certificates issued | Demonstrate PK including multipl key storage med required for ente |
| | Personnel requisition submission and processing<br>**Pilot pending** | **City of Norfolk** | **CA:** DIT<br>**Product:** Verisign | Demonstrate we manage person multiple signatu |
| G 2 B | Interagency transfer of funds<br>**Plan to move into production environment**<br>**Pilot pending** | **Virginia Information Providers Network (VIPNet)**<br>· DMV<br>· VIPNet Authority Board<br>· VIPNet Authority Board Executive Committee<br>· Virginia Interactive, LLC<br>· DIT Fiscal staff | **CA:** Served as own CA<br>**Product:** Entrust<br>10 certificates issued | Use of digital sig authorization for |
| | Electronic bidding for VDOT contracts<br>**Will move to production environment** | **Virginia Department of Transportation**<br>· Virginia Road and Transportation Builders Association<br>· Industry representatives<br>· Federal Highway Administration Representative | **CA:** InfoTech, Inc.<br>**Products:** Expedite, Bid Express<br>11 certificates issued | Demonstrate ele Proposals (RFP secured system |
| | Electronic Procurement | **Department of General Services (DGS)**<br>· Vendors (North Carolina and Massachusetts)<br>· James River Correctional Center Purchasing Department<br>· Division of Purchases & Supply | **CA:** VIPNet<br>**Product:** Entrust<br>14 certificates issued | To evaluate the and digital signa This was accom form electronica authorization of documents post emailed to supp |

# DIGITAL SIGNATURE INITIATIVE DELIVERABLES

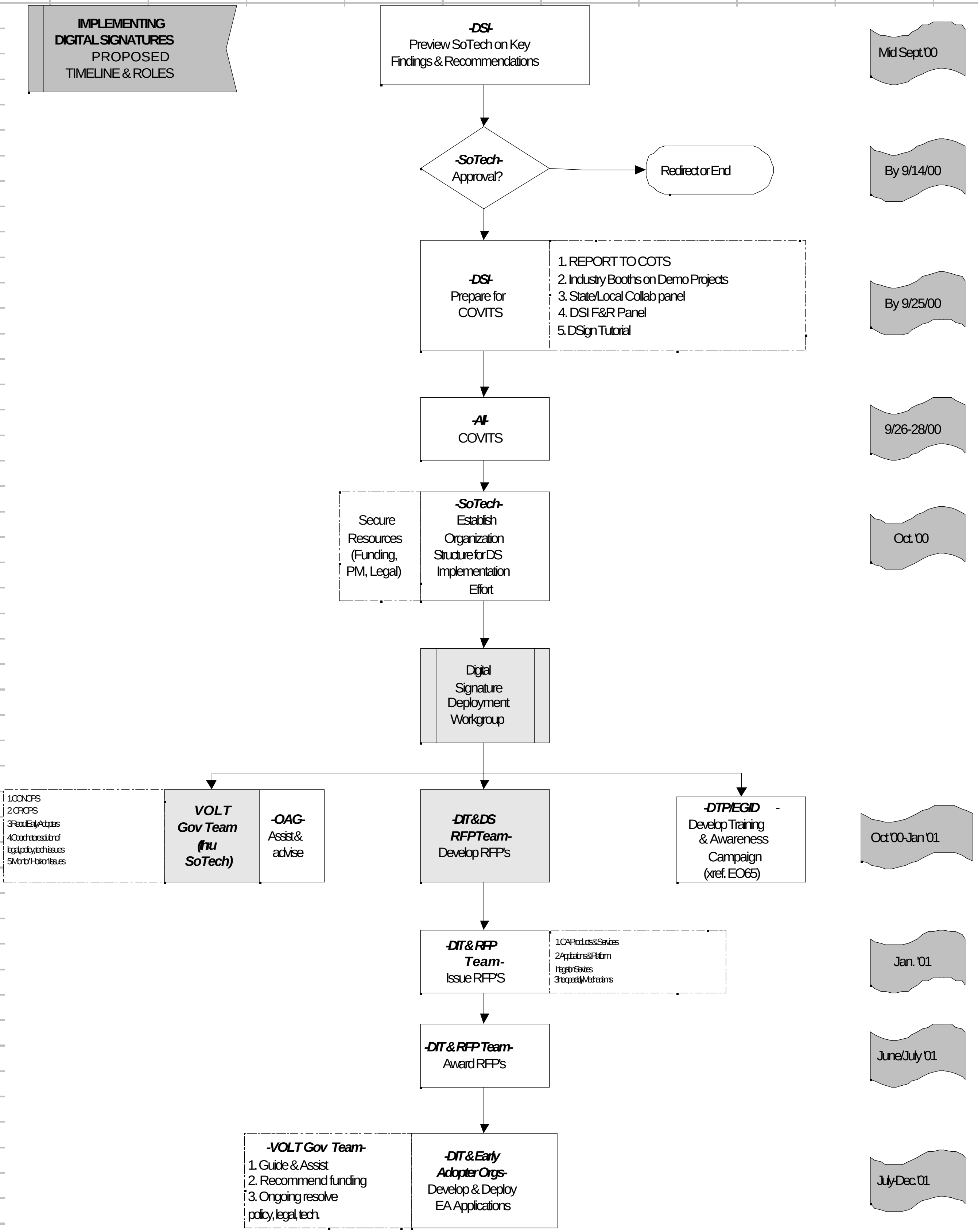
## COTS/PSA REPORT RELATED TO EXECUTIVE ORDERS 51 & 65

| COTS/PSA DIGITAL SIGNATURE REPORT · 10/99 | | EXECUTIVE ORDER 51 · 7/23/99 | | EX |
|---|---|---|---|---|
| DELIVERABLES (6) | COMP. | DELIVERABLE S | COMP. | |
| — N/A — | | The Secretary of Technology shall submit a report to the Governor by 11/1/99 concerning plan to facilitate the use and authentication of electronic signatures. (I.) | ✓ | |
| Establish the Digital Signature Initiative Workgroup to demonstrate use of digital signatures internally within an agency, agency to agency, agency to business partners, and agency to local government, and to report on results. (6) | ✓ | — N/A — | | The Secreta coordinate v Technology developmer standards, a statewide d signatures. |
| -N/A- | | -N/A- | | The Secreta receive adv COTS in reg implementa demonstrati |
| A demonstrated working ***solution of trust*** and confidence extensible to the Commonwealth public sector community, to business partners and to the public. (5) | | — N/A — | | Developmer model that a digital signa extended to sector comr and to the g |
| A Commonwealth Bridge Certification Architecture. (3) | | — N/A — | | Developmer structure tha more than c |
| An enterprise technical architecture and acquisition strategy based on experience. (2) | | — N/A — | | Application environmen secure digit could later b |
| A foundation of policies, practices, guidelines and standards necessary to transition into an enterprise production environment. (1) | | — N/A — | | Establishme guidelines t applying dig |

| COTS/PSA DIGITAL SIGNATURE REPORT · 10/99 | | EXECUTIVE ORDER 51 · 7/23/99 | | EX |
|---|---|---|---|---|
| DELIVERABLES (6) | COMP. | DELIVERABLE S | COMP. | |
| An invested knowledge and skills base for decision makers and technical staff. (4) | | -N/A- | | |
| -N/A- | | -N/A- | | The Secreta encourage a Branch age advantage o technology. |
| | | — N/A — | | The Secreta develop an agencies, in education, a how to impl signature te |
| — N/A — | | — N/A — | | The Secreta coordinate w Executive B the procure statewide d signature te |
| — N/A — | | — N/A — | | The Secreta ensure that signature te Commonwe provisions o Transaction |
| -N/A- | | -N/A- | | The Govern agencies ar advantage o signature te possible. |
| — N/A — | | Agencies must incorporate guidance from the Sec. of Technology on use of electronic signature technology into their proposed plans for Web-enabled internal/external transactions. (J.) | | |

# DSI TIME-PHASED WORKPLAN

EXHIBIT F



# DSI TIME-PHASED WORKPLAN

EXHIBIT F